Présentation du 9e rapport annuel

par Denis Beau, Président
et Julien Lasalle, Secrétaire

Conférence de presse du 9 septembre 2025

bservatoire
de la sécurité
des moyens de paiement
www.observatoire-paiements.fr

6 focus sur les points saillants du rapport annuel 2024

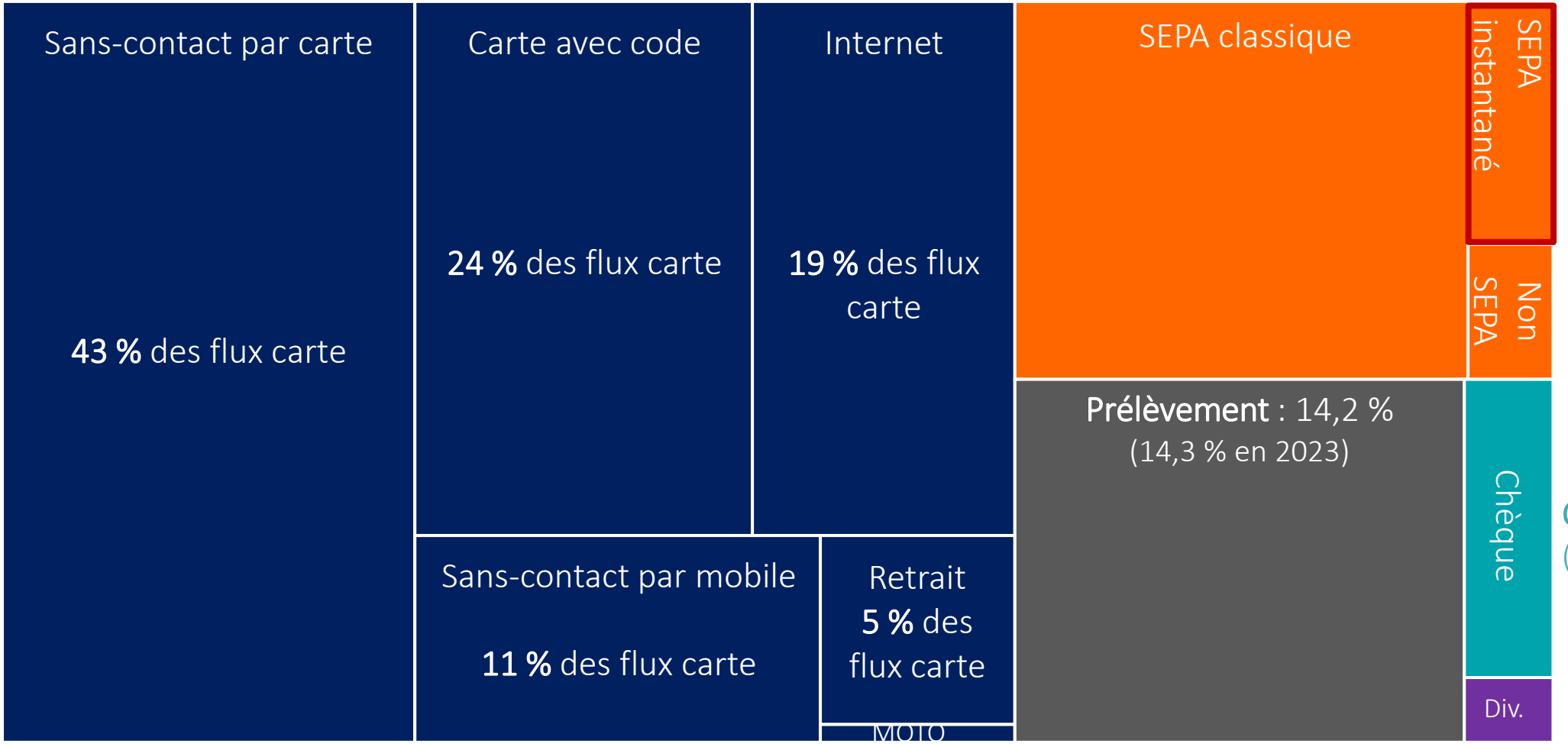
1. L'usage des moyens de paiement en 2024
2. L'évolution de la fraude et des principaux modes opératoires
3. Les priorités d'**actions de prévention de la fraude**
4. Les travaux de **veille technologique** sur l'intelligence artificielle
5. Le bilan des recommandations sur le remboursement de la fraude
6. La sensibilisation des utilisateurs, un priorité permanente

❶ L'usage des moyens de paiement scripturaux en 2024

33,8 milliards d'opérations (+5,2 %) | Montants échangés : 34 864 Md€ (+3,4 %)

Opérations par carte : 65,1 % (64,6 % en 2023)

Virement : 17,7 % (17,6 % en 2023)



10 % des virements émis

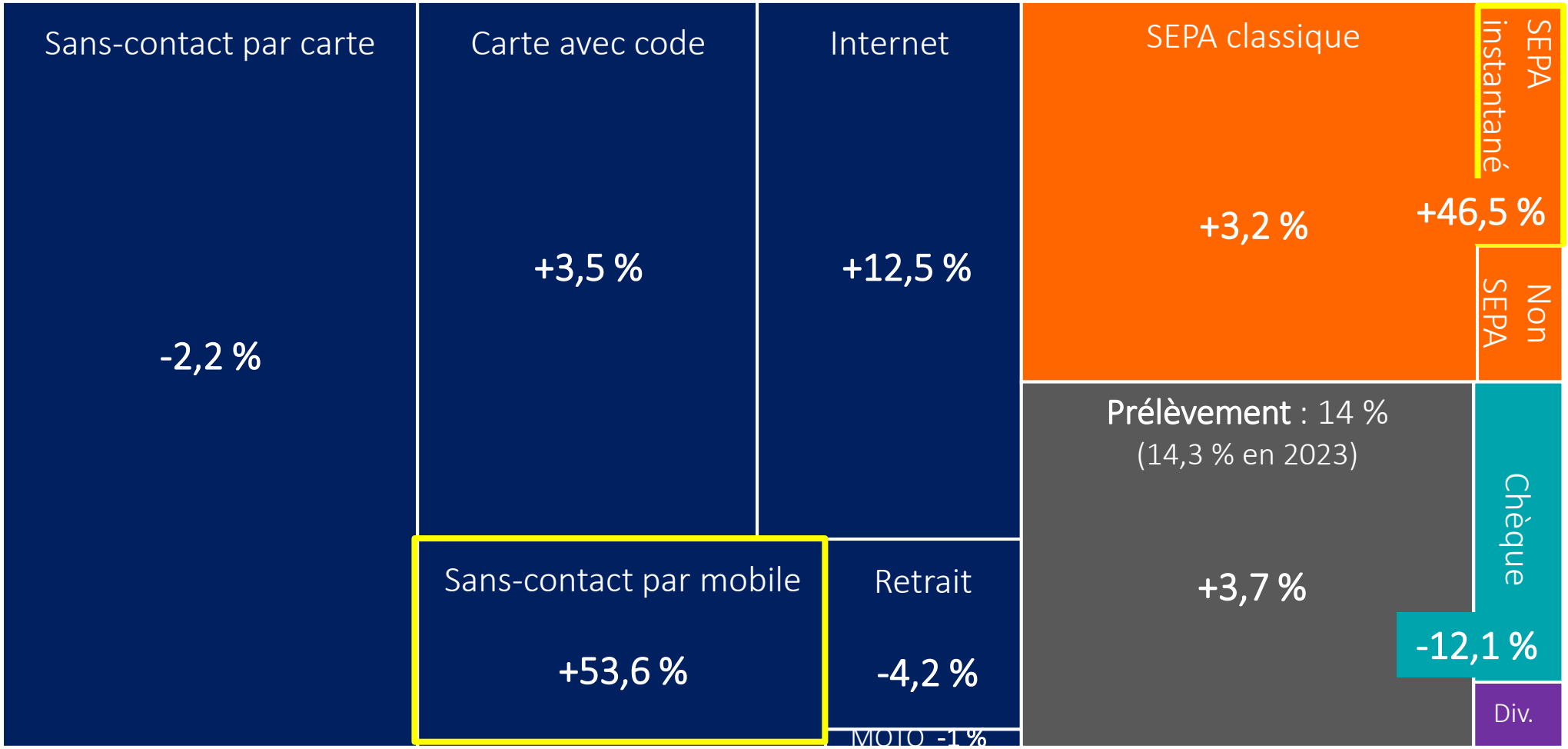
Chèque : 2,3 %
(2,8 % en 2023)

❶ L'usage des moyens de paiement scripturaux en 2024

33,8 milliards d'opérations (+5,2 %) | Montants échangés : 34 864 Md€ (+3,4 %)

Opérations par carte : 65,1 % (64,6 % en 2023)

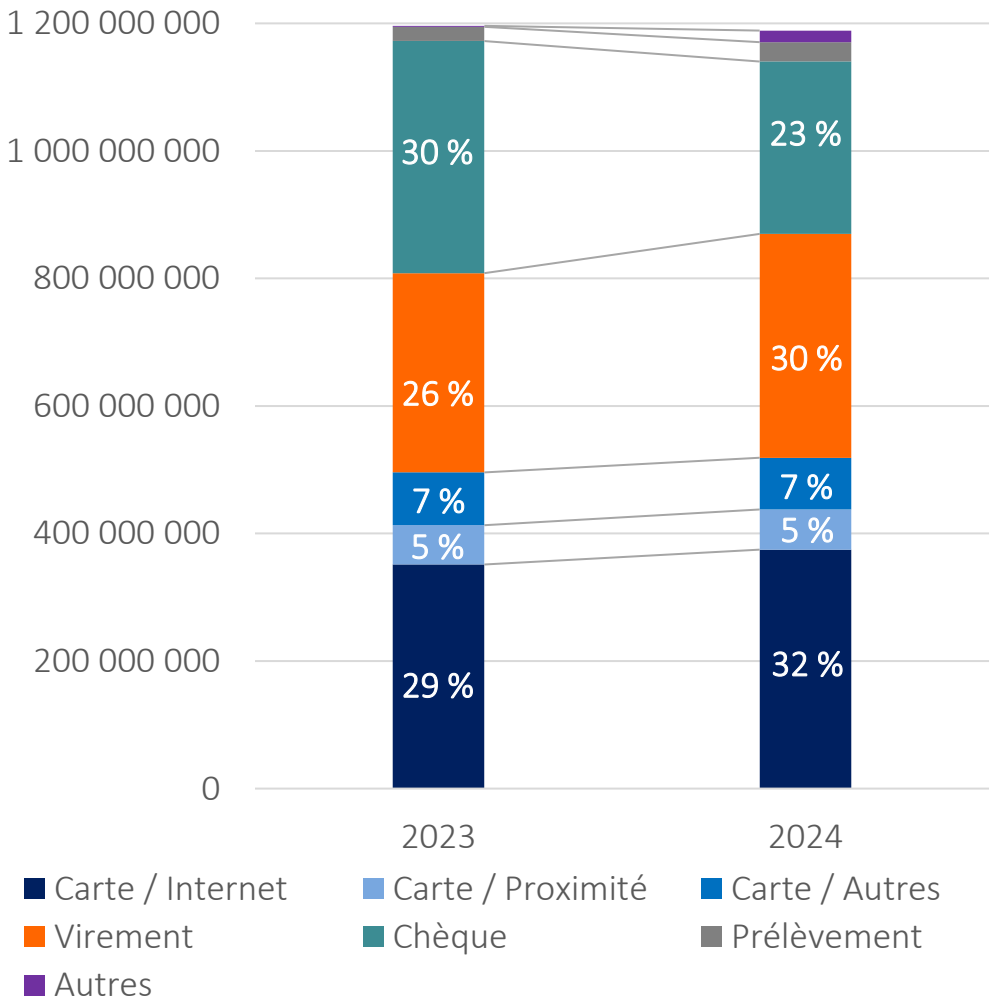
Virement : 17,7 % (17,6 % en 2023)



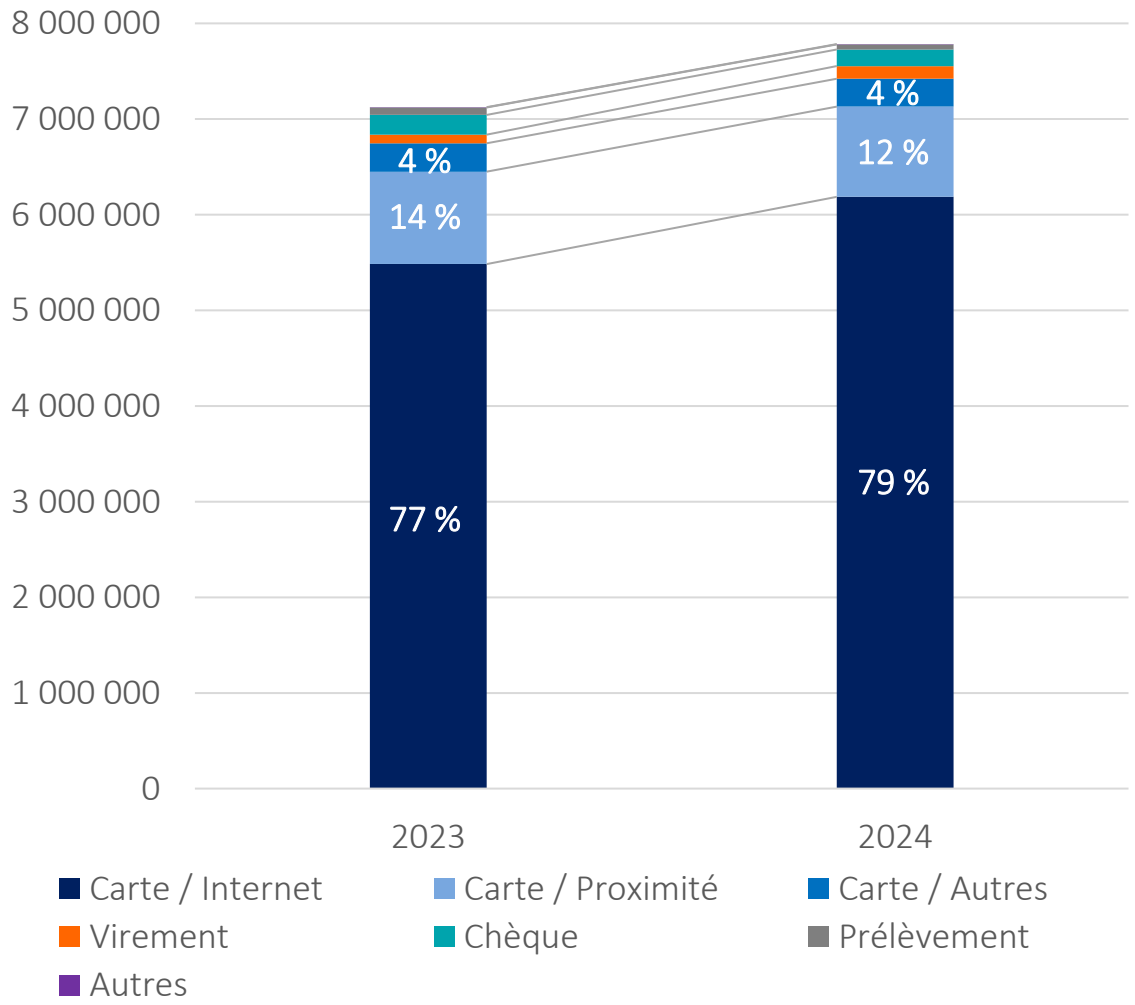
Chèque : 2,3 %
(2,8 % en 2023)

❷ La fraude aux moyens de paiement scripturaux en 2024

1,19 Milliard d'€, en baisse de -0,6 % sur un an

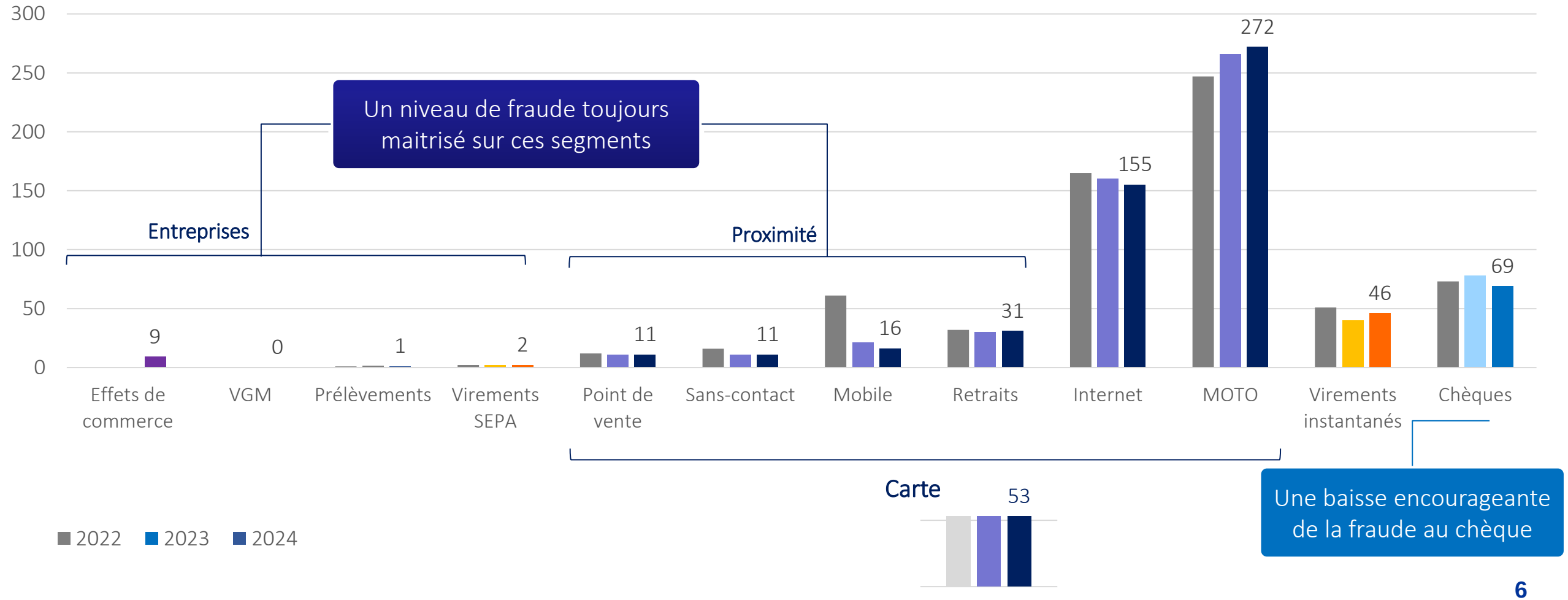


7,8 millions de cas de fraude, en hausse de +9,3 %



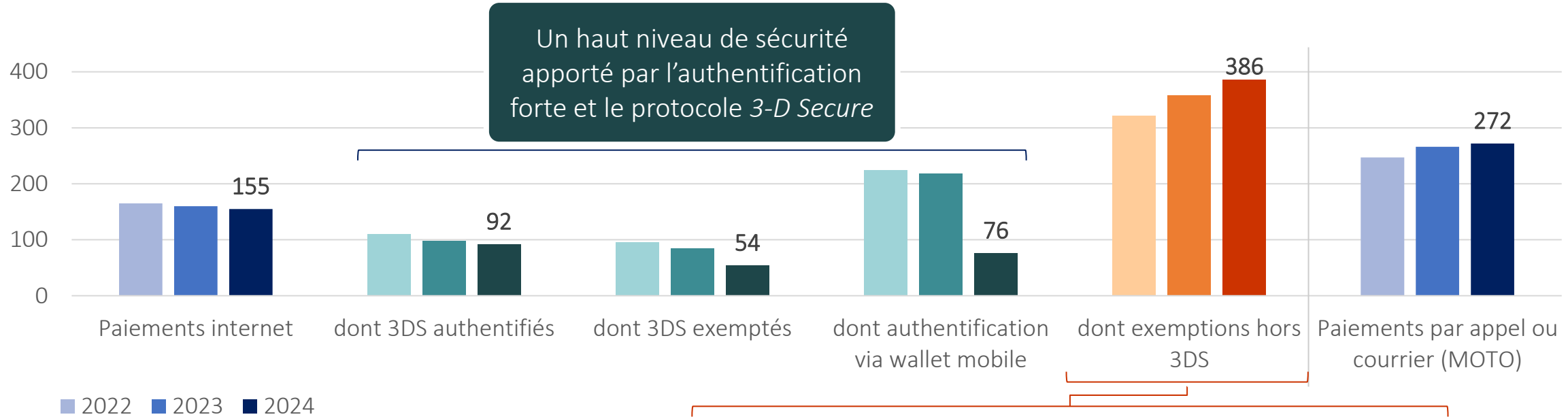
❷ Évolution de la vulnérabilité des canaux de paiement à la fraude

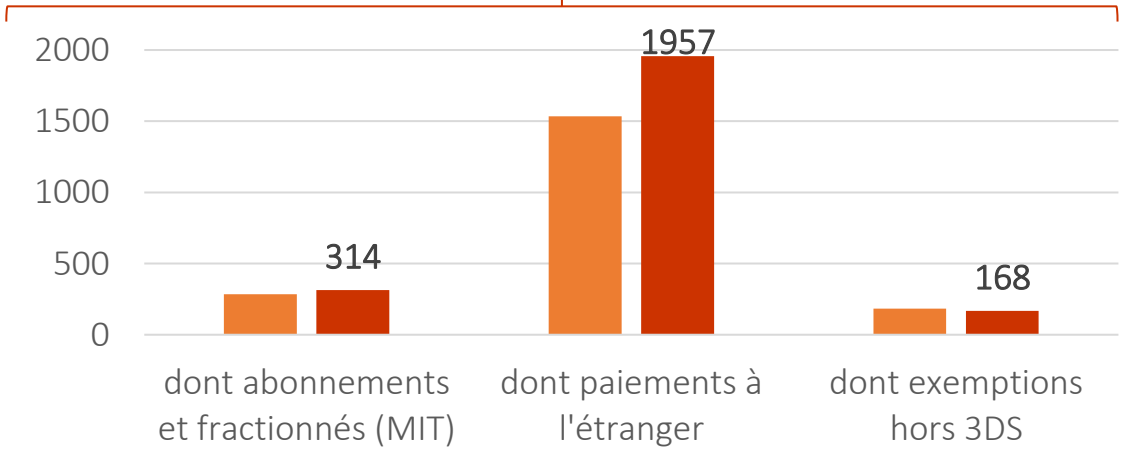
en € de fraude / 100.000 € de paiements



❷ Évolution de la vulnérabilité des canaux de paiement à la fraude

Focus sur les paiements carte à distance (en € de fraude / 100.000 € de paiements)





Les paiements non authentifiés / non *3-D Secure* (43 % des paiements à distance mais seulement 2,8 % des montants) sont particulièrement exposés à la fraude

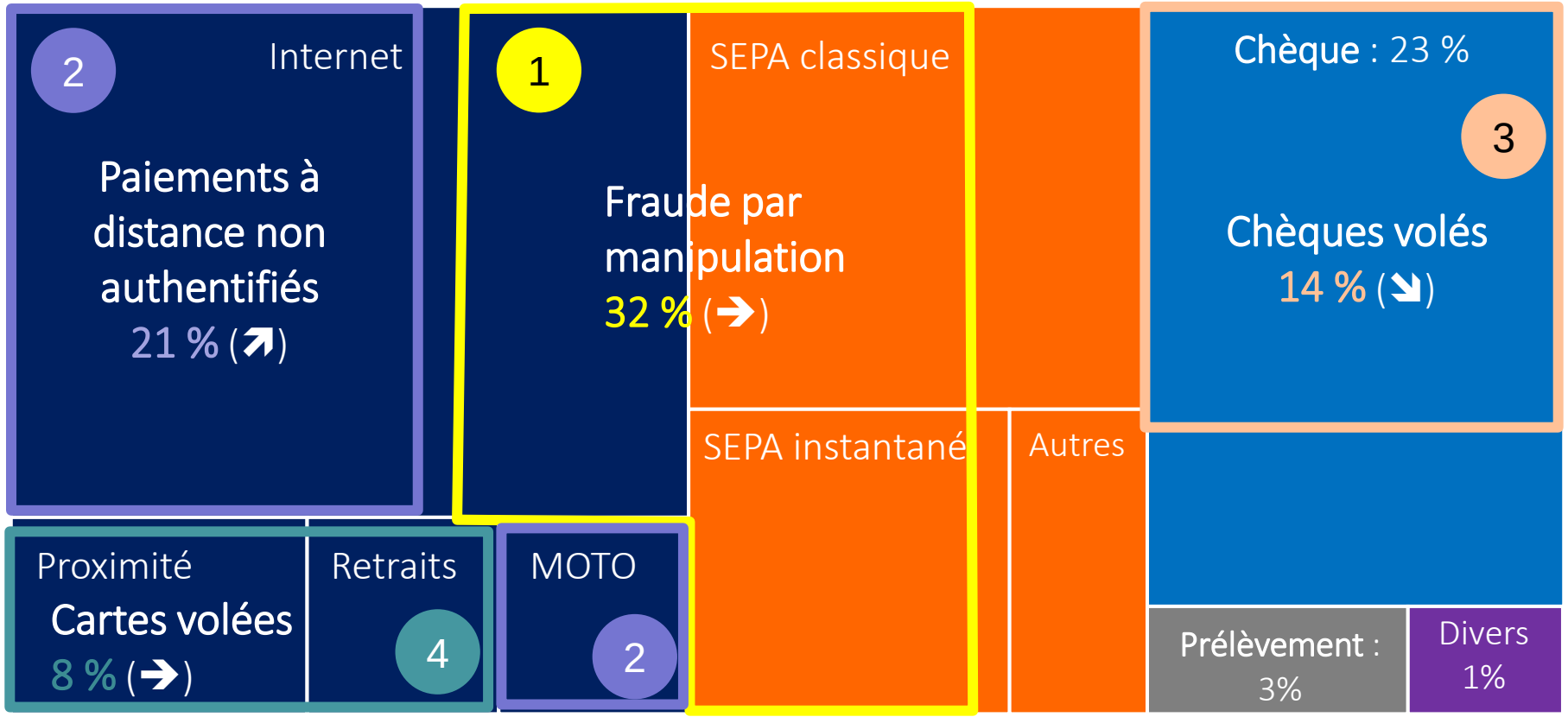
❷ Les principaux types de fraude en 2024

4 modes opératoires qui concentrent 75 % du montant de la fraude

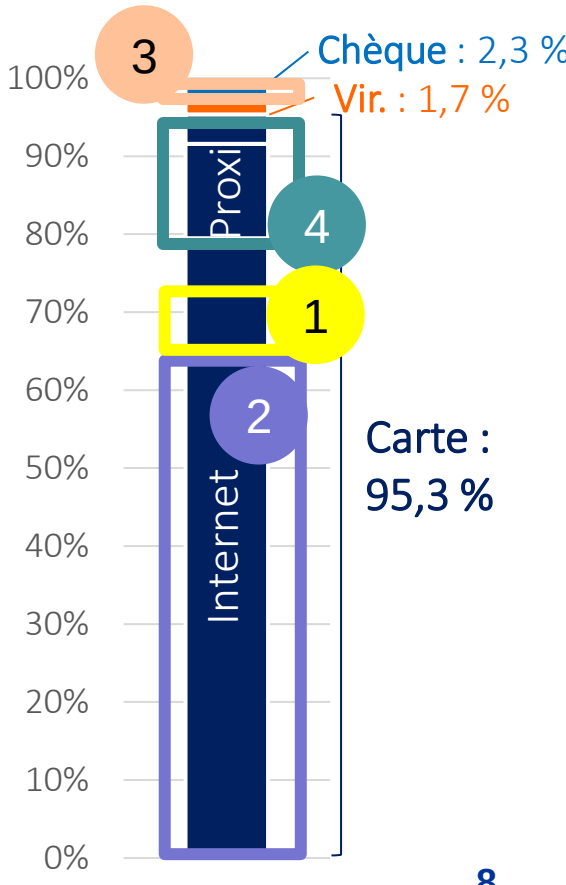
1,19 Milliard d'€, en baisse de -0,6 % sur un an

Opération par carte : 44 %

Virement : 30 %

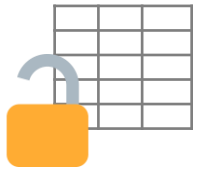


7,8 millions de cas
en hausse de +9,3 %



❸ Lutte contre la fraude par manipulation

Des actions centrées sur la sécurisation des canaux de communication



Collecte de données de paiement et personnelles

- Hameçonnage
- Sites miroirs
- Réseaux sociaux

Fraude aux paiements sécurisés par **usurpation** (faux conseiller bancaire)

Les réalisations qui permettent de contenir la fraude

Déploiement du mécanisme d'authentification des numéros

Modernisation et valorisation du 33700 pour lutter contre le *smishing*

Protection des identifiants d'envoi de SMS

API de suivi des réémissions de cartes SIM

Les pistes complémentaires à l'étude

Implication des plateformes numériques dans les mécanismes de détection et de signalement

Sécurisation des outils de communication avec les clients

Facilitation du partage de données de fraude entre établissements

❸ Sécurisation des paiements par carte à distance hors 3DS

Des actions pour restreindre le recours aux canaux peu sécurisés

Paiements par courrier ou appel téléphonique (MOTO)

« Prélèvements » par carte (MIT)

Paiements internet non authentifiés hors 3DS (CIT - DTA)

Les réalisations qui permettent de contenir la fraude

Limitations des paiements :
- 500 € pour les MOTO
- 1 € pour les CIT-DTA
- Rejet de tout MIT non assorti d'une référence de mandat authentifié

Exemptions spécifiques pour certains secteurs d'activité dépendant des MOTO

Mesures ciblées portant sur les 10 commerçants exemptés les plus exposés à la fraude

Les pistes complémentaires à l'étude

Abaissement des seuils de limitation des paiements y compris pour les secteurs exemptés et poursuite du ciblage des commerçants exposés

Extension aux flux internationaux en fonction du degré de maturité et de l'exposition à la fraude

Soutien au développement de solutions d'authentification forte adaptées (TO) et de traçabilité des mandats (MIT)

❸ Actions de l'Observatoire pour limiter la fraude au chèque

3 priorités pour sécuriser les usages résiduels du chèque

Réduire les risques associés à la distribution des chéquiers

- Mise à disposition des chéquiers en agence sans surcoût
- **Alerte et renforcement de la traçabilité des envois par voie postale**

Renforcer l'efficacité des mises en opposition des chèques volés

- **Simplicité de la mise en opposition sans formalisme excessif**
- Frais de mise en opposition proportionnés et sans renouvellement

Lutter contre les remises frauduleuses de chèques

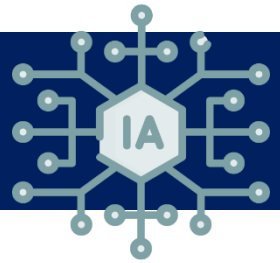
- Renforcement des mécanismes d'identification et de temporisation des remises atypiques
- Actions de sensibilisation des utilisateurs

- **Gratuité des mises en opposition en cas de non-réception des chéquiers**

L'Observatoire rappelle qu'**il ne faut jamais accepter d'encaisser un chèque pour compte d'autrui** : c'est à la fois **dangereux** et **illégal** !

❹ Étude de veille sur l'informatique artificielle

Risques et opportunités pour la sécurité des paiements



L'intelligence artificielle dans le domaine des paiements : un nouveau terrain d'affrontement pour la sécurité des paiements

Des opportunités pour les professionnels des paiements par l'évaluation en temps réels du niveau de risque des transactions…

Facilitation du recours aux exemptions à l'authentification forte pour les transactions peu risquées

Meilleure identification des opérations à risque et mise en œuvre de mesures de sécurité complémentaires

… et des opportunités pour les fraudeurs via de nouvelles capacités de création offertes par l'IA générative

Industrialisation des campagnes de collecte de données par génération de sites miroirs, traduction automatique…

Renforcement des capacités d'usurpation d'identité par *deep fake* (audio, voire vidéo)

❹ Étude de veille sur l'informatique artificielle

Les recommandations de l'Observatoire pour préparer l'avenir

Objectif: améliorer la qualité des données tout au long de la chaîne des paiements pour maximiser le potentiel de l'IA

Évaluer au niveau de chaque acteur l'opportunité **d'expérimenter des technologies d'intelligence artificielle** dans leurs dispositifs d'analyse des risques

Valoriser l'ensemble des données exploitables dans les dispositifs d'analyse de risque, en veillant à la qualité et à l'exhaustivité des données échangées dans les messages de paiement et en y intégrant les mécanismes de partage de Place

Évaluer de façon régulière l'efficacité des modèles de *scoring* intégrant des modules d'IA en termes de performance, d'intelligibilité et d'explicabilité

❺ Bilan des recommandations sur le remboursement de la fraude

Principaux enseignements (1/2)

Des apports très significatifs de l'application des recommandations en matière de prévention de la fraude

Une **meilleure information** apportée au client tout au long du parcours de paiement, couplée à des **campagnes régulières de sensibilisation** au risque de fraude

L'**introduction de frictions et d'options** visant à contrer les tentatives de manipulation dans les parcours d'authentification

Des **pistes d'amélioration** identifiées au sein de certains PSP en termes de gestion des risques (nouveau terminal utilisé) ou d'offre proposée au client (listes blanches ou noires)

Une plus grande capacité de vigilance et de résistance apportée à l'utilisateur, qui a contribué à contenir la fraude par manipulation directe

❺ Bilan des recommandations sur le remboursement de la fraude

Principaux enseignements (2/2)

Des progrès significatifs en matière de traitement des réclamations, avec des points d'amélioration attendus

Un **traitement désormais conforme** à l'esprit des recommandations

✓ Analyse et justifications fondées sur les critères recommandés par l'Observatoire

✓ Abandon des exigences de formalisme excessives (signature, remise d'un dépôt de plainte…)

✗ Des progrès encore attendus de certains PSP sur la restitution de justificatifs

Des **taux de remboursement de qualification et de remboursement globalement cohérents** :

✓ Les cas de litiges commerciaux et de contestations abusives représenteraient ¼ des réclamations

✗ Un taux de remboursement très insuffisant sur les virements sans authentification forte (20 % contre 98 % pour les cartes)

De façon générale, le renforcement des parcours client apporte également davantage d'éléments d'analyse au PSP dans le traitement des réclamations

❻ La sensibilisation des utilisateurs, une priorité permanente

3 réflexes pour se prémunir contre la fraude

(Ne pas) réagir face aux contacts non sollicités (mails, SMS, publicités…)

- Ne donnez jamais d'information personnelle ou sensible après redirection
- Contactez si besoin votre interlocuteur par des canaux habituels et sûrs
- Signalez les messages non sollicités (33700, outils de blocage de votre messagerie…)

Ne jamais valider d'opération dont on n'est pas à l'origine

- Un conseiller bancaire n'a pas besoin de votre intervention pour bloquer un paiement douteux
- En cas de sollicitation de ce type, rappelez immédiatement votre conseiller bancaire

Ne jamais encaisser de chèque qui ne vous est pas destiné

- … même si vous pensez connaître la personne qui vous le demande
- C'est illégal et dangereux !

❻ La sensibilisation des utilisateurs, une priorité permanente

Ce qui va changer le 9 octobre avec la « vérification du bénéficiaire »

L'introduction d'une vérification interbancaire systématique de la concordance entre les informations saisies pour valider le bénéficiaire d'un virement

Nom du bénéficiaire :	Archimède Pi
IBAN du bénéficiaire :	GR 3 1415 9265 3589 793

Vérification dans la base de clientèle par l'établissement teneur du compte

- Concordance parfaite : poursuite du paiement
- Concordance quasi-parfaite : affichage du nom corrigé pour validation
- Non-concordance : alerte à l'utilisateur l'invitant à vérifier les informations

➔ Une protection majeure contre la fraude par substitution d'IBAN

❻ La sensibilisation des utilisateurs, une priorité permanente

L'Observatoire résolument engagé

… et une nouvelle campagne à venir fin 2025 …

N° INCONNU + APPROCHE NON SOLLICITÉE = DANGER !

BONS RÉFLEXES :
RACCROCHER | SUPPRIMER | SIGNALER

En 2024-2025 dans la presse, à la radio et sur internet…

… sur différents supports, y compris affichage public

Présentation du 9e rapport annuel

par Denis Beau, Président
et Julien Lasalle, Secrétaire

Conférence de presse du 9 septembre 2025

bservatoire
de la sécurité
des moyens de paiement
www.observatoire-paiements.fr